



IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : **Confirmation No. 4485**

Masato YAMAMICHI et al. : Docket No. 2003\_1741A

Serial No. 10/725,208 : Group Art Unit 2131

Filed December 2, 2003 :

KEY AGREEMENT SYSTEM,  
SHARED-KEY GENERATION APPARATUS,  
AND SHARED-KEY RECOVERY  
APPARATUS :

THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEES FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975

**INFORMATION DISCLOSURE STATEMENT**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Pursuant to the provisions of 37 CFR 1.56, 1.97 and 1.98, Applicants request consideration of the references listed on attached form PTO-1449 and any additional information identified below in paragraph 3. A legible copy of each reference listed on the Form PTO-1449 is enclosed, except a copy is not provided for:

- ☐ each U.S. Patent and U.S. Patent application publication;
- ☐ each reference previously cited in the international application  
PCT/\_\_\_\_\_; and/or
- ☐ each reference previously cited in prior parent application Serial No.  
\_\_\_\_\_.

1a. [X] This Information Disclosure Statement is submitted:

within three months of the filing date (or of entry into the National Stage) of the above-entitled application, **or**

before the mailing of a first Office Action on the merits or the mailing of a first Office Action after the filing of an RCE,

**and thus no certification and/or fee is required.**

1b. ☐ This Information Disclosure Statement is submitted

after the events of above paragraph 1a and prior to the mailing date of a final Office Action or a Notice of Allowance or an action which otherwise closes prosecution in the application, and thus:

(1) ☐ the certification of paragraph 2 below is provided, **or**

(2) ☐ the fee of \$180.00 specified in 37 CFR 1.17(p) is enclosed.

1c. ☐ This Information Disclosure Statement is submitted:

after the mailing date of a final Office Action or Notice of Allowance or action which otherwise closes prosecution in the application, and prior to payment of the issue fee, and thus:

**the certification of paragraph 2 below is provided, and**

**the fee of \$180.00 specified in 37 CFR 1.17(p) is enclosed.**

2. It is hereby certified

a. ☐ that each item of information contained in this Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Statement, or

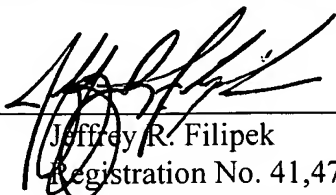
b. ☐ that no item of information contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the person signing the certification after making reasonable inquiry, was known to any individual designated in §1.56(c) more than three months prior to the filing of the Statement.

3. ☐ Consideration of the following list of additional information (including any copending or abandoned U.S. application, prior uses and/or sales, etc.) is requested.
4. For each non-English language reference listed on the attached form PTO-1449, reference is made to:
- a. ☐ a full or partial English language translation submitted herewith,
  - b. ☐ a foreign patent office search report (in the English language) submitted herewith,
  - c. ☐ the concise explanation contained in the specification of the present application at page,
  - d. ☐ the concise explanation set forth in the attached English language abstract,
  - e. ☐ the concise explanation set forth below or on a separate sheet attached to the reference:
5. ☒ A foreign patent office search report citing one or more of the references is enclosed.
6. ☐ Statement Under 37 CFR 1.704(d)

Each item of information contained in the Information Disclosure Statement was first cited in any communication from a foreign Patent Office in a counterpart application, and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement.

Respectfully submitted,

Masato YAMAMICHI et al.

By   
Jeffrey R. Filipek  
Registration No. 41,471  
Attorney for Applicants

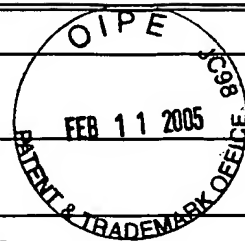
JRF/fs  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
February 11, 2005

## INFORMATION DISCLOSURE STATEMENT

FORM PTO 1449 (modified)

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICELIST OF REFERENCES CITED BY APPLICANT(S)  
(Use several sheets if necessary)

Date Submitted to PTO: February 11, 2005

ATTY DOCKET NO.  
2003\_1741ASERIAL NO.  
10/725,208APPLICANT  
Masato YAMAMICHI et al.FILING DATE  
December 2, 2003GROUP  
2131

## U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						

## FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES NO
	AJ						
	AK						
	AL						

## OTHER DOCUMENT(S) (Including Author, Title, Date, Pertinent Pages, Etc.)

AM	Howgrave-Graham et al., "The Impact of Decryption Failures on the Security of NTRU Encryption", Advances in Cryptology- Crypto 2003, 23 <sup>rd</sup> Annual International Cryptology Conference, Santa Barbara, CA, August 17-21, 2003 Proceedings, Lecture Notes in Computer Science, vol. 2729, Berlin, Springer, DE, August 17, 2003, pages 226-243
AN	EESS: Consortium for Efficient Embedded Security: "Efficient Embedded Security Standards #1: Implementation Aspects of NTRUEncrypt and NTRUSign. Draft Version 2.0", EESS-Consortium for Efficient Embedded Security, 'Online! June 2003, pages 1-78
AO	Institute of Electrical and Electronics Engineers, Inc.: "Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices" IEEE Draft Standard P1363.1-D2, 'Online! May 18, 2001, pages 1-38
AP	Menezes, Oorschot, Vanstone: "Handbook of Applied Cryptography", CRC Press Series on Discrete Mathematics and Its Applications, 1997, pages 506-508, 551, 552, 359-362, Boca Raton, FL, US

EXAMINER

DATE CONSIDERED